(19) JAPANESE PATENT OFFICE

Reference 3

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10013784 A**

(43) Date of publication of application: **16.01.98**

(51) Int. Cl **H04N 5/91**
H04L 9/18
H04L 9/30
H04N 7/167

(21) Application number: **08163137**

(22) Date of filing: **24.06.96**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

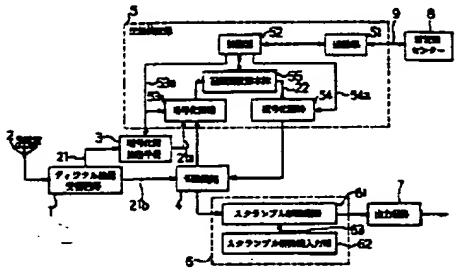
(72) Inventor: **MAEDA TAKIO**

(54) **BROADCAST SIGNAL RECORDING AND REPRODUCING DEVICE**

(57) Abstract

PROBLEM TO BE SOLVED: To attain charge imposition every time a recorded broadcast signal is reproduced by providing a key acquisition means to acquire a decoding key externally.

SOLUTION: A communication section 51 as a key acquisition means makes communication with a key management center 8 when a broadcast signal recording reproducing device reproduces program recording data to receive a ciphering key 53a and a decoding key 54a. When the key management center 8 sends the ciphering key 53a and the decoding key 54a to a communication section 51, charge is imposed onto a viewer making the transmission request. A decoding circuit 54 uses the decoding key 54a to decode program recording data to be outputted and reproduced from a recording device main body 55, a ciphering circuit 53 uses a new ciphering key 53a to cipher again the signal outputted from the decoding circuit 54 and the result is outputted to the recording device main body 55. Thus, every time same program recording data are decoded, the data are ciphered by a new key and then rewritten.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－13784

(43)公開日　平成10年(1998)１月16日

(51)Int.Cl.⁶		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｈ０４Ｎ	5/91			Ｈ０４Ｎ	5/91	Ｚ	
Ｈ０４Ｌ	9/18			Ｈ０４Ｌ	9/00	６５１	
	9/30					６６３Ｚ	
Ｈ０４Ｎ	7/167			Ｈ０４Ｎ	7/167	Ｚ	

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平8－163137

(22)出願日　平成８年(1996)６月24日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　前田　多吉生
大阪府門真市大字門真1006番地　松下電器産業株式会社内

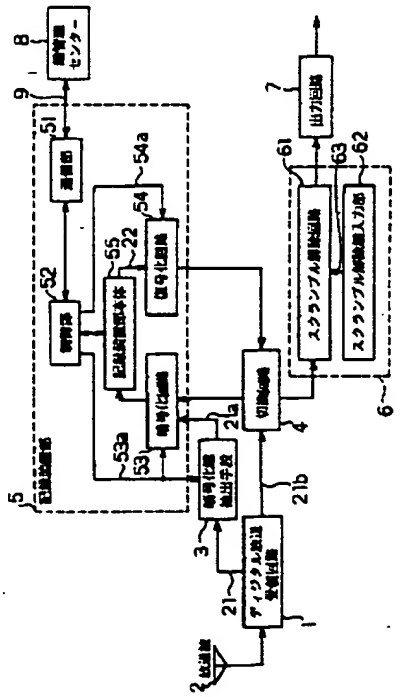
(74)代理人　弁理士　松田　正道

(54)【発明の名称】　放送信号記録再生装置

(57)【要約】

【課題】一旦記録された番組の視聴の度に課金をすることは出来ないと言う課題

【解決手段】放送信号を受信するディジタル放送受信回路１と、受信信号を暗号化鍵により暗号化する暗号化回路５３と、その暗号化された暗号化信号を記録媒体に記録する記録装置部本体５５と、記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得する通信部５１と、その取得された復号化鍵を用いて、記録された暗号化信号を復号する復号化回路５４と、その復号化された信号を再生し、出力する出力回路７等を備える。



1

【特許請求の範囲】

【請求項１】　放送信号を受信する受信手段と、
前記受信信号を暗号化鍵により暗号化する暗号化手段と、
その暗号化された暗号化信号を記録媒体に記録する記録手段と、
前記記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得する鍵取得手段と、
その取得された復号化鍵を用いて、前記記録された暗号化信号を復号する復号化手段と、
その復号化された信号を再生し、出力する再生・出力手段と、を備えたことを特徴とする放送信号記録再生装置。

【請求項２】　前記暗号化鍵は、公開鍵暗号系の公開鍵であり、前記復号化鍵は、その公開鍵に対応する秘密鍵であることを特徴とする請求項１記載の放送信号記録再生装置。

【請求項３】　前記鍵取得手段は、前記復号化鍵を取得する際に、再記録用の暗号化鍵も取得し、
前記暗号化手段は、前記復号化手段が前記復号を行う場合、その復号化された前記記録信号を前記再記録用の暗号化鍵を用いて再度暗号化し、
前記記録手段は、その再度暗号化された暗号化信号を前記記録媒体に更新記録することを特徴とする請求項１又は、２記載の放送信号記録再生装置。

【請求項４】　前記受信信号を暗号化する暗号化鍵は、前記放送信号に含まれており、
前記放送信号から前記暗号化鍵を抽出する暗号化鍵抽出手段を備え、
前記暗号化手段は、その抽出された暗号化鍵を用いることを特徴とする請求項１～３の何れか一に記載の放送信号記録再生装置。

【請求項５】　前記受信信号を暗号化する暗号化鍵を予め格納する鍵格納手段を備え、
前記暗号化手段は、その格納された暗号化鍵を用いることを特徴とする請求項１～３の何れか一に記載の放送信号記録再生装置。

【請求項６】　前記暗号化手段は、前記鍵取得手段により取得された前記再記録用の暗号化鍵を、前記受信信号の暗号化に用いることを特徴とする請求項３記載の放送信号記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送信号記録再生装置に関するものである。

【０００２】

【従来の技術】従来より、有料テレビ放送としてＣＡＴＶや衛星放送などが知られている。また、この様な、有料テレビ放送のシステムにおいては、放送信号に妨害信号を重畳して、著作権を保護する方法が知られている。

2

そして、著作権を保護する機能を有する記録装置として、「特開平７－１５４３８５　妨害重畳情報処理装置」等が開示されている。

【０００３】以下、著作権を保護する機能を有する妨害重畳情報処理装置の構成を動作を、図３を用いて同時に説明する。

【０００４】図３に示す様に、アンテナ１０１から得られたディジタルテレビ放送信号は、暗号化された信号であり、ディジタル放送受信回路１０７で受信される。この受信信号は、記録機器１１０に内蔵された記録部１１２によって、記録媒体１１３に暗号化されたままの状態で記録される。この様にして記録された放送信号を再生する場合は、再生部１１４からの再生出力が、専用のデコーダーボックス１２０の入力端子１１６を通して、選択回路１０８へ送られる。ユーザが、リアルタイムで放送を視聴する場合は、選択回路１０８は、ディジタル放送信号回路１０７からの出力信号を選択し、暗号解除回路１１７へ出力する。又、ユーザが、記録機器１１０に記録された信号を視聴する場合は、選択回路１０８は、記録機器１１０からの出力信号を選択して、暗号解除回路１１７へ出力する。暗号解除回路１１７に送られた、放送信号あるいは、記録信号は、復号化された後、視聴可能な状態に再生されると言う構成である。尚、上記暗号化は、放送局毎、即ち、放送チャンネル毎に異なる暗号化が行われている。

【０００５】従って、記録装置１１０により記録されている放送信号は、専用のデコーダーボックス１２０を用いて、チャンネル毎に異なる暗号解除鍵により解除しない限り、視聴可能な状態には再生されない。即ち、これにより、放送信号を記録できても、専用のデコーダーボックス１２０が無い限り再生が出来ないため、著作権の保護が可能となる。

【０００６】

【発明が解決しようとする課題】しかしながら、上記の様な従来の記録再生装置では、専用のデコーダーボックスを備えておりさえすれば、一旦記録した映像データを繰り返し、何度でも視聴することが可能であり、そのような自由な視聴を制限することが出来ないと言う問題点を有していた。

【０００７】即ち、従来の記録再生装置を前提とした有料放送システムは、チャンネル毎の課金しか出来ず、一旦記録された番組の視聴の度に課金をすることは出来ないと言った課題があった。

【０００８】本発明は、従来の記録再生装置のこのような課題を考慮し、記録された放送信号を再生する毎に課金が出来得る放送信号記録再生装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】請求項１記載の本発明は、放送信号を受信する受信手段と、前記受信信号を暗

号化鍵により暗号化する暗号化手段と、その暗号化された暗号化信号を記録媒体に記録する記録手段と、前記記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得する鍵取得手段と、その取得された復号化鍵を用いて、前記記録された暗号化信号を復号する復号化手段と、その復号化された信号を再生し、出力する再生・出力手段とを備えた放送信号記録再生装置である。

【００１０】請求項２記載の本発明は、前記暗号化鍵は、公開鍵暗号系の公開鍵であり、前記復号化鍵は、その公開鍵に対応する秘密鍵である放送信号記録再生装置である。

【００１１】請求項３記載の本発明は、前記鍵取得手段は、前記復号化鍵を取得する際に、再記録用の暗号化鍵も取得し、前記暗号化手段は、前記復号化手段が前記復号を行う場合、その復号化された前記記録信号を前記再記録用の暗号化鍵を用いて再度暗号化し、前記記録手段は、その再度暗号化された暗号化信号を前記記録媒体に更新記録する放送信号記録再生装置である。

【００１２】請求項４記載の本発明は、前記受信信号を暗号化する暗号化鍵は、前記放送信号に含まれており、前記放送信号から前記暗号化鍵を抽出する暗号化鍵抽出手段を備え、前記暗号化手段は、その抽出された暗号化鍵を用いる放送信号記録再生装置である。

【００１３】請求項５記載の本発明は、前記受信信号を暗号化する暗号化鍵を予め格納する鍵格納手段を備え、前記暗号化手段は、その格納された暗号化鍵を用いる放送信号記録再生装置である。

【００１４】請求項６記載の本発明は、前記暗号化手段は、前記鍵取得手段により取得された前記再記録用の暗号化鍵を、前記受信信号の暗号化に用いる放送信号記録再生装置である。

【００１５】請求項１記載の本発明では、受信手段が放送信号を受信し、暗号化手段が前記受信信号を暗号化鍵により暗号化し、記録手段がその暗号化された暗号化信号を記録媒体に記録し、鍵取得手段が前記記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得し、復号化手段がその取得された復号化鍵を用いて、前記記録された暗号化信号を復号し、再生・出力手段がその復号化された信号を再生し、出力する。

【００１６】請求項２記載の本発明では、前記暗号化鍵は、公開鍵暗号系の公開鍵であり、前記復号化鍵は、その公開鍵に対応する秘密鍵である。

【００１７】請求項３記載の本発明では、前記鍵取得手段は、前記復号化鍵を取得する際に、再記録用の暗号化鍵も取得し、前記暗号化手段は、前記復号化手段が前記復号を行う場合、その復号化された前記記録信号を前記再記録用の暗号化鍵を用いて再度暗号化し、前記記録手段は、その再度暗号化された暗号化信号を前記記録媒体に更新記録する。

【００１８】請求項４記載の本発明では、前記受信信号を暗号化する暗号化鍵は、前記放送信号に含まれており、暗号化鍵抽出手段が、前記放送信号から前記暗号化鍵を抽出し、前記暗号化手段は、その抽出された暗号化鍵を用いる。

【００１９】請求項５記載の本発明では、鍵格納手段が、前記受信信号を暗号化する暗号化鍵を予め格納し、前記暗号化手段は、その格納された暗号化鍵を用いる。

【００２０】請求項６記載の本発明では、前記暗号化手段は、前記鍵取得手段により取得された前記再記録用の暗号化鍵を、前記受信信号の暗号化に用いる。

【００２１】これにより、例えば、記録された放送信号を再生する毎に復号化鍵が必要となる。

【００２２】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。

【００２３】図１は、本発明の一実施の形態の放送信号記録再生装置の構成図、図２（ａ）は、ディジタル放送信号のデータ構成を説明する図であり、同図を参照しながら、本実施の形態の構成を説明する。

【００２４】即ち、図２（ａ）において、本実施の形態のディジタル放送信号２１は、各放送番組毎に異なる公開鍵暗号系の公開鍵２１ａを、その番組データ２１ｂと共に、各放送局から送信される信号である。ここで、番組データ２１ｂは、放送局において予めスクランブル化されている。図１に示すように、本発明の受信手段としてのディジタル放送受信回路１は、アンテナ２から得られたディジタル放送信号２１を受信し、その受信信号から番組データ２１ｂを分離して、後述する制御部５２の指示を得て出力する回路手段である。暗号化鍵抽出手段３は、ディジタル放送受信回路１が受信したディジタル放送信号２１から、公開鍵２１ａを抽出し、後述する暗号化回路へ出力する手段である。切換回路４は、放送信号等の流れを切り換えるための回路である。記録装置部５は、番組データ２１ｂを暗号化して記録媒体（図示省略）に記録し、あるいは、その記録媒体に記録された番組記録データ２２を再度別の暗号化鍵を用いて更新記録する他、それら番組記録データ２２を復号化するためのものである。スクランブル解除部６は、記録装置部５により復号化された信号のスクランブル状態を解除するためのものである。又、本発明の再生・出力手段としての出力回路７は、スクランブル解除部６からの出力を得て、表示・出力部（図示省略）等へ再生信号として出力する手段である。

【００２５】記録装置部５は、通信部５１、制御部５２、暗号化回路５３、復号化回路５４及び記録装置部本体５５を備えている。本発明の鍵取得手段としての通信部５１は、本実施の形態の放送信号記録再生装置の外部に設けられている鍵管理センター８と、電話回線９を介して接続されている。通信部５１は、放送信号記録再生装置において番組記録データ２２が再生される場合に、

鍵管理センター８と通信を行い、暗号化用の鍵５３ａと復号化用の鍵５４ａとを受け取る手段である。鍵管理センター８は、通信部５１へ暗号化用の鍵５３ａと復号化用の鍵５４ａを送信した際に、その送信要求をしてきた視聴者に対して、課金を行うものである。暗号化用の鍵５３ａは、番組記録データ２２を、後述する更新記録のために再度暗号化する際に用いられる公開鍵暗号系の公開鍵であり、復号化用の鍵５４ａは、番組記録データ２２を復号化する際に用いられる公開鍵暗号系の秘密鍵である。制御部５２は、通信部５１が得た暗号化用の鍵５３ａと復号用の鍵５４ａとをそれぞれ分離して、前者を暗号化回路５３へ送り、後者を復号化回路５４へ送る他、暗号化鍵抽出手段３に対して、公開鍵２１ａを暗号化回路５３へ転送するタイミング等を指示する手段である。又、制御部５２は、後で詳細に述べるが、通信部５に対して、通信部５が鍵管理センター８から、適切な鍵をもらうために必要な鍵情報を送る手段である。本発明の暗号化手段としての暗号化回路５３は、ディジタル放送受信回路１から出力された番組データ２１ｂを暗号化する場合には、暗号化鍵抽出手段３から出力された公開鍵２１ａを用い、又、一旦記録された番組記録データ２２を、更新記録のために再度暗号化する場合には、上記暗号化用の鍵５３ａを用いる手段である。本発明の記録手段としての記録装置部本体５５は、記録媒体としてハードディスクを内蔵し、暗号化回路５３からの暗号化信号をその暗号化に用いた鍵と共に記録する手段である。本発明の復号化手段としての復号化回路５４は、番組記録データ２２を、制御部５２から出力された復号化用の鍵５４ａを用いて、復号化するための手段である。

【００２６】ここで、重要なことは、制御部５２から出力された復号化用の鍵５４ａは、その復号化の対象となる番組記録データ２２が、暗号化された際に用いられた鍵に対応する鍵でなければならない点である。そのため、視聴者が番組記録データ２２を再生しようとする場合、制御部５２は、記録装置部本体５５に対して、記録された番組記録データ２２の中から、視聴者が再生指示した番組記録データと対にして記録されている、暗号化に用いられた鍵を調べさせて、その鍵の鍵情報を通信部５へ伝える。

【００２７】スクランブル解除部６は、スクランブル解除回路６１と、スクランブル解除鍵入力部６２を備えている。スクランブル解除回路６１は、スクランブル解除鍵入力部６２から得られたスクランブル解除鍵６３を用いて、復号化回路５４からのスクランブル化された状態の出力信号に対して、そのスクランブル状態を解除するための回路である。

【００２８】以上ような構成において、図１を主に参照しながら、本実施の形態の動作を説明する。

（１）先ず、リアルタイムで、放送番組を視聴する場合について述べる。

【００２９】図１に示すように、ディジタル放送受信回路１により分離された番組データ２１ｂは、切換回路４を介して、スクランブル解除回路６１へ送られる。スクランブル解除回路６１は、スクランブル解除鍵入力部６２から入力された鍵を用いて、そのスクランブル状態を解除して、出力回路７へ出力する。出力回路７はスクランブル状態の解除された番組データ２１ｂを表示・出力装置へ出力する。

【００３０】これにより、視聴者は、放送されている番組をリアルタイムで見ることが出来る。

（２）次に、番組を記録し、それを再生する場合について述べる。

【００３１】（２－１）先ず、ディジタル放送受信回路１から出力されたリアルタイムの番組データ２１ｂを記録する場合を説明する。

（ステップ１０１）ディジタル放送受信回路１により分離された番組データ２１ｂは、切換回路４を介して、暗号化回路５３へ送られる。

（ステップ１０２）暗号化鍵抽出手段３は、ディジタル放送信号２１から抽出した公開鍵２１ａを、制御部５２からの指示に基づいて、暗号化回路５３へ送る。

（ステップ１０３）暗号化回路５３は、上記公開鍵２１ａを用いて、番組データ２１ｂを暗号化し、その暗号化に用いた公開鍵２１ａと共に記録装置部本体５５へ出力する（図２（ｂ）参照）。ここで、図２（ｂ）は、公開鍵２１ａにより暗号化された番組記録データ２２と、その公開鍵２１ａとにより構成された記録データを模式的に表した図である。

（ステップ１０４）記録装置部本体５５は、図２（ｂ）に示すように、暗号化された番組データ２１ｂとその暗号化に用いた公開鍵２１とを対にして、ハードディスクに記録する。

【００３２】（２－２）次に、一旦ハードディスクに記録された記録番組データ２２を再生する場合を説明する。

（ステップ２０１）視聴者から記録番組データを再生する旨の再生指示があった場合、制御部５２は、記録装置部本体５５に対して、視聴者が指示した再生すべき番組記録データ２２（図２（ｂ）参照）を、ハードディスク内で検索させる。そして、番組記録データ２２に対応して記録されている、暗号化に用いられた鍵の鍵情報を通信部５へ伝える。

（ステップ２０２）通信部５１は、制御部５２から送られてきた鍵情報を、鍵管理センター８へ送る。鍵管理センター８は、自ら保持する鍵の中から、その鍵情報に基づいて、対応する復号化用の鍵５４ａを選び出し、記録装置部本体５５が交信記録に用いる暗号化用の鍵５３ａと共に、通信部５１へ送信する。

（ステップ２０３）制御部５２は、通信部５１に送られた上記２種類の鍵の内、上記復号化用の鍵５４ａを復号

化回路５４へ送り、上記暗号化用の鍵５３ａを暗号化回路５３へ送る。復号化回路５４は、その復号化用の鍵５４ａを用いて、記録装置部本体５５から出力される再生すべき番組記録データ２２を復号化し、切換回路４へ出力する。

（ステップ２０４）切換回路４は、復号化回路５４からの復号化済みの信号がスクランブル解除回路６１と暗号化回路５３とに同時に送られる様に、接続状態を切り換える。

（ステップ２０５）スクランブル解除回路６１に送られた復号化済みの信号は、既に（１）で説明した、リアルタイムで、放送番組を視聴する場合と同様にして、スクランブル状態が解除されて、出力回路７へ出力される。

（ステップ２０６）一方、これと同時に、暗号化回路５３は、上述した様に通信部５１が取得した新たな暗号化用の鍵５３ａを用いて、復号化回路５４から出力されてきた信号を、再び暗号化して記録装置部本体５５へ出力する（図２（ｃ）参照）。ここで、図２（ｃ）は、新たな鍵５３ａにより暗号化された番組記録データ２２と、その鍵５３ａとにより構成された記録データを模式的に表した図である。

（ステップ２０７）記録装置部本体５５は、図２（ｃ）に示すように、再度暗号化された信号を新たな鍵５３ａと共に、更新記録する。

【００３３】以上のことから、同じ番組記録データ２２が、復号化の度に、新たな鍵によって暗号化され、その都度書き換えれることになる。従って、次に、同じ番組記録データ２２を再生しようとする場合、必ず、新しい復号化用の鍵を鍵管理センター８からもらい、その新しい鍵で復号化しない限り、再生は不可能となる。これにより、鍵管理センター８は、視聴者が番組記録データを再生する度に、課金することが出来る。

【００３４】尚、上記実施の形態では、暗号化の度に暗号化用の鍵を変える場合について説明したが、これに限らず例えば、常に同じ鍵を用いて暗号化してもよく、要するに、記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得する構成でありさえすればよい。

【００３５】又、上記実施の形態では、復号化用の鍵は、暗号化用の鍵に対応してその都度変わる場合について説明したが、これに限らず例えば、常に同じ復号化用の鍵を用いて復号化してもよく、要するに、記録された暗号化信号の復号化に用いられる復号化鍵を外部から取得する構成でありさえすればよい。この場合、復号化用の鍵は、復号化に使用した後は、メモリー等に保持しないで常に消去する構成にしておくことが望ましい。放送信号記録再生装置を改造して、メモリー等に保持された復号化用の鍵を、記録データの復号化に不正に使用することを防止するためである。

【００３６】又、上記実施の形態では、暗号化を行うための鍵を、暗号化の対象となるデータに応じて、使い分ける場合について説明したが、これに限らず例えば、鍵取得手段により取得された再記録用の暗号化鍵を、受信信号の暗号化にも兼用する構成でももちろんよい。

【００３７】又、上記実施の形態では、暗号化を行うための鍵を、ディジタル放送信号２１の中からと、外部の鍵管理センターからの二通りのルートから得る場合について説明したが、これに限らず例えば、受信信号を暗号化する暗号化鍵を予め格納する鍵格納手段を備え、暗号化手段は、その格納された暗号化鍵を用いて、受信信号を暗号化する構成でもよい。この場合、再記録用の暗号化鍵を、外部から取得する構成としてもよいし、あるいは、再記録自体を行わない構成としてもよい。再記録を行わない場合は、暗号化鍵を外部から取得する必要はもちろんない。

【００３８】

【発明の効果】以上のように本発明によれば、記録された放送信号を再生する毎に課金が出来得るという長所を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態による放送信号記録再生装置の構成図

【図２】（ａ）：ディジタル放送信号のデータ構成の模式図

（ｂ）：暗号化された番組記録データ等を模式的に表した図

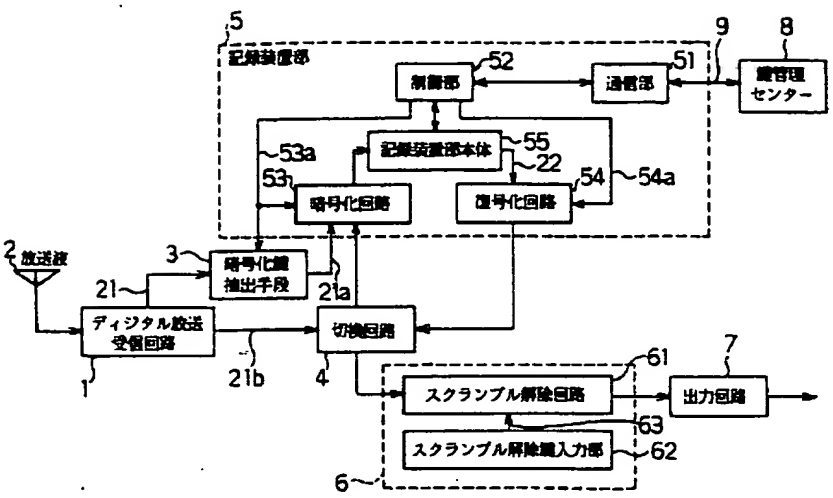
（ｃ）：別の暗号化鍵により暗号化された番組記録データ等を模式的に表した図

【図３】従来の妨害重畳情報処理装置の構成図

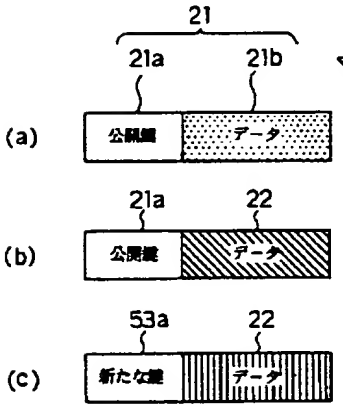
【符号の説明】

１	ディジタル放送受信回路
２	アンテナ
３	暗号化鍵抽出手段
４	切換回路
５	記録装置部
６	スクランブル解除部
７	出力回路
２１	ディジタル放送信号
２１ａ	公開鍵
２１ｂ	番組データ
２２	番組記録データ
５２	制御部

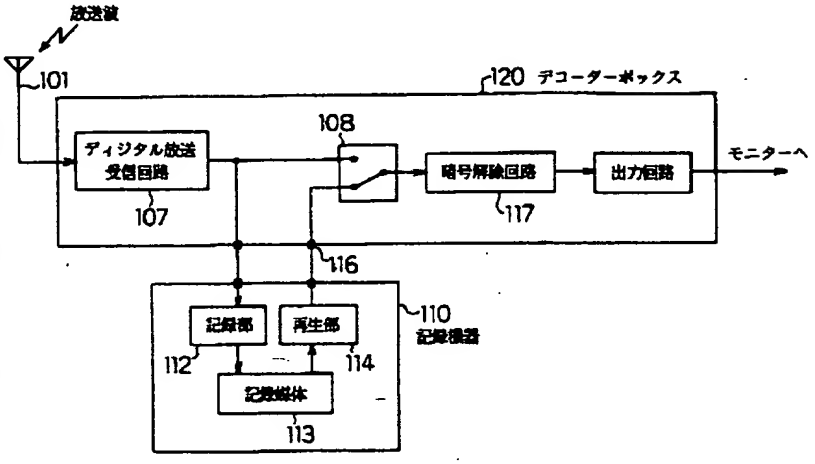
【図１】


5
記録装置部
9
8
52
51
通信部
鍵管理センター
53a
記録装置部本体
55
22
53
54
54a
暗号化回路
復号化回路
2
放送波
3
暗号化鍵抽出手段
21
21a
ディジタル放送受信回路
切換回路
1
21b
4
61
7
スクランブル解除回路
出力回路
63
スクランブル解除鍵入力部
62
6

【図２】


21
21a
21b
(a)
公開鍵
データ
21a
22
(b)
公開鍵
データ
53a
22
(c)
新たな鍵
データ

【図３】


放送波
101
120 デコーダーボックス
108
ディジタル放送受信回路
107
暗号解除回路
117
出力回路
モニターへ
116
110
記録機器
記録部
再生部
112
114
記録媒体
113